## REMARKS

Claims 1-11, 16, 17, 28 and 33-41 have been cancelled. Claims 12 and 25 have been amended. New claims 42 and 43 have been added to round out the scope of protection afforded the invention. Applicants reserve the right to pursue the original claims and other claims in this application and other applications. Claims 12-15, 18-27, 29-32, 42 and 43 are pending in this application.

The Specification was objected to because of informalities. The Specification has been amended to address the Examiner's concerns.

Claim 39 stands rejected under 35 U.S.C. 112, second paragraph, as being indefinite. Claim 39 has been cancelled.

Claims 1-8, 10, 11 and 33-41 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Leon (US 6,424,954). Claims 9, 12, 16-25 and 28-32 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Leon in view of Schneier (US 5,956,404). Claims 13-15, 26 and 27 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Leon in view of Schneier and further in view of Mosher (US 5,799,322). Reconsideration is respectfully requested.

As noted in the current specification, in many instances it is desirable, or in some cases mandated by the postal authority, for value dispensing devices, e.g., postage meters, to maintain usage information. Such usage information can include, for example, the amount of postage dispensed by the meter, as well as other data, including, for example, total mail piece counts, piece counts for different classes of mail, piece counts for each different postage amount dispensed, etc. The usage information is typically compiled over a predetermined period of time, referred to as an audit period, such as, for example, weekly, monthly, or yearly. At the end of the determined audit period, the captured data for that audit period is transmitted to a data center, such as, for example, a data center operated by the meter manufacturer, where it is used to prepare reports. The prepared reports can be sent to the postal authority. These reports may then be utilized by the postal authorities (or the meter manufacturer) for such things, for example, as statistical analysis of use of the meter population, customer billing, etc.

There are problems, however, with conventional systems and methods for preparing data capture reports for a given audit period. One such problem is that the data capture data is blindly trusted for preparation of a report. The data capture data, however, may not be fully trustworthy when received from the postage meter. For example, since the usage information is not securely stored within the device, it is possible for a dishonest person to modify the data capture data before it is transmitted to the meter manufacturer. For example, the value of the total amount of postage dispensed during the audit period could be modified in such a way that this value is made lower than the actual value used. In cases where the reports are used for billing purposes, the postal authority would under bill the customer, based on the modified data capture report, and thus the postal authority would be defrauded of funds due.

The present invention alleviates the problems associated with the prior art and provides a system and method that can detect tampering with data capture data, as well as verify the authenticity of data capture data, in a value dispensing system. At the beginning of an audit period, an audit record is generated by the postage meter that includes the current register values at the beginning of the audit period and a digital signature generated by the device. At the end of the audit period, a second audit record is generated by the postage meter that includes the register values at the end of the audit period and a digital signature generated by the device. This end of period audit record is then transmitted to the data center, along with the data capture data and the start of period audit record (if not previously transmitted to the data center). The data center, after obtaining both the end of period audit record and start of period audit record, will verify the digital signature of the both audit records. Successful verification of the digital signatures authenticates the device to the data center, and indicates that the register values are valid, as any modification of the data contained within the audit records would result in a failure of the signature verification. The data center can then reconcile the postage meter usage, i.e., register values, by comparing the difference between the register values from the start of period audit record and the end of period audit record with the values as contained within the data capture data for the audit period. Any discrepancies between these values indicate that the data capture data may not be correct, and a further investigation can be performed. If there are no discrepancies, the data capture data is deemed to be accurate and the data can be utilized to prepare reports with a high degree of certainty that it accurately reflects the actual usage of the postage meter. (See Specification, paragraphs [0022] through [0025]).

In view of the above, claim 12 as amended is directed to a method for a data center to process usage data of a value dispensing device that comprises "receiving a first audit record from the value dispensing device, the first audit record generated by the value dispensing device at a start of an audit period, the first audit record including a value of at least one register maintained by the value dispensing device at the start of the audit period and a first digital signature; receiving a second audit record from the value dispensing device, the second audit record generated by the value dispensing device at an end of the audit period, the second audit record including a value of the at least one register maintained by the value dispensing device at the end of the audit period and a second digital signature; receiving usage data from the value dispensing device for the audit period; verifying the first and second digital signatures; if the first and second digital signatures verify, determining a difference between the value of the at least one register at the end of the audit period and the start of the audit period; comparing the determined difference with corresponding data provided in the usage data; and if the determined difference correlates with the corresponding data provided in the usage data, generating a usage report for the value dispensing system based on the usage data."

Leon, in contrast is directed to a postage metering system in which an audit transaction is performed periodically to reset a timer. If the timer times out before an audit transaction is performed, the secure metering device (SMD) transitions to a state in which no further operation (except for an audit transaction) is permitted. A user requests an audit causing the host PC to send an audit request message to the SMD. The SMD then sends the host PC a signed message that includes the required information, which can include the current contents of the secure revenue registers, the device ID number, the current date and time, and a transaction serial number generated by the SMD. The host PC forwards the signed message to a system server, which receives and validates the message. As part of the processing, the system server authenticates the signed message using the SMD's public key and analyzes the data included in the message. The system server then sends the host PC a signed message that includes the response data, including the same device ID and transaction number from the message received earlier. The host PC forwards this signed message to the SMD, which validates the message by verifying the signature and determining if the message is of an expected type. If the signature is valid and the message is of an expected typed, the SMD determines if the data contents of the message is correct by verifying the transaction serial number. If the data is valid, the SMD resets the timer and transitions to an operating state. (Col. 18, line 30 to Col. 19, line15).

Thus, in Leon the system uses only a single audit record for the purpose of resetting a timer. There is no disclosure, teaching or suggestion in Leon of "receiving a second audit record from the value dispensing device, the second audit record generated by the value dispensing device at an end of the audit period, the second audit record including a value of the at least one register maintained by the value dispensing device at the end of the audit period and a second digital signature" as is recited in claim 12. In Leon, there is no second audit record generated at the end of an audit period. The system in Leon uses only a single audit record taken at a specific point in time.

There is also no disclosure, teaching or suggestion in Leon of "determining a difference between the value of the at least one register at the end of the audit period and the start of the audit period" or "comparing the determined difference with corresponding data provided in the usage data" as is recited in claim 12. The audit record in Leon is used to reset a timer, and there is no determination of a difference between values of a register at the end of and audit period and the start of the audit period, or of a comparison of any difference to usage data. There is also no disclosure, teaching or suggestion in Leon of generating a usage report for the value dispensing system based on the usage data if the determined difference correlates with the corresponding data provided in the usage data as is recited in claim 12.

The reference to Schneier does not cure the above deficiencies. Schneier is directed to providing a strong audit trail for an encryption scheme. In Schneier, a signature packet includes message bits, which are formed by hashing a message, auditing bits, and redundancy bits for the security of the signature. The auditing bits may be used to trace the identity of the source generating the message, and may also be used to trace the sequence of events or transactions operated on by the device token by including a packet-sequence number, which increments every time the device token generates a signature. Other auditing bits that can trace the sequence of events is bits representing the hashing of the immediate prior signature signed by the card. This would provide an audit trail where every signature includes its immediately prior signature, making it difficult for an intruder to change such type of audit trail because every previous signature would have to be changed. (Col. 3, line 65 to Col. 4, line 21).

Thus, Schneier provides a digital signature in which an audit trail for the signature is provided. There is no disclosure, teaching or suggestion in Schneier of "receiving a first audit record from the value dispensing device, the first audit record generated by the value dispensing device at a start of an audit period, the first audit record including a value of at least one register maintained by the value dispensing device at the start of the audit period and a first digital signature; receiving a second audit record from the value dispensing device, the second audit record generated by the value dispensing device at an end of the audit period, the second audit record including a value of the at least one register maintained by the value dispensing device at the end of the audit period and a second digital signature; receiving usage data from the value dispensing device for the audit period; verifying the first and second digital signatures; if the first and second digital signatures verify, determining a difference between the value of the at least one register at the end of the audit period and the start of the audit period; comparing the determined difference with corresponding data provided in the usage data; and if the determined difference correlates with the corresponding data provided in the usage data, generating a usage report for the value dispensing system based on the usage data."

Neither of the cited references, either alone or in combination, disclose, teach or suggest all of the limitations of the present invention as detailed above. For at least the above reasons, Applicants respectfully submit that claim 12 as amended is allowable over the prior art of record. Claims 13-15, 18-24 and 42, dependent upon claim 12, are allowable along with claim 12 and on their own merits.

Claim 25 as amended includes limitations similar to those of claim 12. For the same reasons given above with respect to claim 12, Applicants respectfully submit that claim 25 is allowable over the prior art of record. Claims 26, 27, 29-32 and 43, dependent upon claim 25, are allowable along with claim 25 and on their own merits.

In view of the foregoing amendments and remarks, it is respectfully submitted that the claims of this case are in a condition for allowance and favorable action thereon is requested.

Respectfully submitted,

/Brian A. Lemm/
Brian A. Lemm
Reg. No. 43,748
Attorney for Applicants
Telephone (203) 924-3836

PITNEY BOWES INC.
Intellectual Property and
Technology Law Department
35 Waterview Drive
P.O. Box 3000
Shelton, CT 06484-8000